ÉÉN JAAR AVG, HOE NU VERDER?

"Heeft uw bedrijf de AVG doelstellingen gehaald?"

Privacy

AVG: één jaar later...

...Het is inmiddels een jaar geleden dat de Algemene Verordening Gegevensbescherming is ingegaan. Wie kan zich niet herinneren dat we op en om 25 mei 2018 vanuit alle hoeken bestookt werden met allerlei e-mails om onszelf opnieuw aan te melden voor diverse nieuwsbrieven? We werden meerdere keren per dag herinnerd aan hoe hoog de boetes zouden zijn (miljoenen!). Een jaar later is de wereld niet vergaan, heeft de bakker om de hoek geen boete gekregen van 20 miljoen euro en mogen bedrijven al sinds oktober 2009 (Telecomwet) niet zonder toestemming een e-mailadres gebruiken voor commerciële doeleinden. Wat is er wel gebeurd? Daarin zullen we u meenemen in deze whitepaper.

Privacy

AVG in een notendop

Sinds 25 mei 2018 is de Algemene Verordening Gegevensbescherming van toepassing. Deze nieuwe privacywetgeving kwam in plaats van de bestaande Wet Bescherming Persoonsgegevens (in Nederland) met richtlijnen die gelden voor alle bedrijven wereldwijd, die persoonsgegevens verwerken van burgers uit de EU. Deze wet is in het leven geroepen vanuit de EU om een daadkrachtige norm voor haar lidstaten te creëren, die wereldwijd gehonoreerd dient te worden.

In Nederland moesten wij eigenlijk al vanaf 1 januari 2016 voor bijna 80% voldoen aan richtlijnen die vergelijkbaar zijn met de AVG. Op die datum is de Wet Bescherming Persoonsgegevens aangescherpt en is de Meldplicht Datalekken in het leven geroepen. Concreet betekent de AVG voor een organisatie dat zij bewust, bekwaam en volgens grondslagen dienen te werken met privacygevoelige informatie. Van elke organisatie wordt verwacht dat zij privacybescherming hoog in het vaandel hebben.

Autoriteit Persoonsgegevens

In het eerste jaar heeft Autoriteit Persoonsgegevens aangegeven alleen boetes op te leggen in uiterste gevallen van ontoelaatbaar gedrag met persoonsgegevens. Inmiddels heeft de Autoriteit Persoonsgegevens niet stilgezeten; maandelijks worden er meerdere artikelen gepubliceerd met handvatten, extra informatie of zelfs toelichting op specifieke gevallen van datalekken. Volgens haar eigen doelstellingen en richtlijnen loopt de Autoriteit Persoonsgegevens nog altijd op schema.

Doordat er nog geen echte jurisprudentie is gerealiseerd, is het lastig om bij deze successtelling aan te sluiten. De Autoriteit Persoonsgegevens dient zich in het tweede jaar daadkrachtiger op te stellen in de handhaving van de AVG.

Het jaarverslag 2018 van Autoriteit Persoonsgegevens:
https://www.autoriteitpersoonsgegevens.nl/nl/nieuws/ap-publiceert-jaarverslag-2018-mijlpaal-voor-privacybescherming

De volgende zaken dient u op orde te hebben om te voldoen aan de AVG-richtlijnen:

- Vastlegging van technische maatregelen die genomen zijn om dataveiligheid en privacy zoveel mogelijk te garanderen.
- Vastlegging van interne processen, procedures en richtlijnen rondom verwerking van persoonsgegevens.
- Het bijhouden van een verwerkingsregister met daarin alle typen persoonsgegevens, locatie van de opslag van persoonsgegevens, de grondslagen van de verwerking op persoonsgegevens en de vastlegging van de verwerkers (derde partijen) welke persoonsgegevens in kunnen zien.
- Het afsluiten van verwerkersovereenkomsten met derde partijen welke persoonsgegevens kunnen inzien.
- Een Datalekregister bijhouden en binnen 72 uur melding maken van een datalek bij de Autoriteit Persoonsgegevens (of tot drie jaar na dato vastleggen waarom er geen melding gemaakt behoefde te worden).

VERWERKINGS REGISTER

Organisaties met minimaal 250 werknemers, organisaties die op grote schaal persoonsgegevens verwerken en organisaties die veel met bijzondere persoonsgegevens werken dienen een verwerkingsregister bij te houden.
Een verwerkingsregister bestaat in elk geval minimaal uit de volgende onderdelen:

- Vastleggen wie (per afdeling, functierol of individu) er met deze persoonsgegevens werken.
- Vastleggen op basis van welke grondslag deze verwerking plaatsvindt.
- Vastleggen op welke (digitale/fysieke) locatie(s) deze persoonsgegevens opgeslagen worden.
- Vastleggen welke verwerkers de organisatie heeft.
- Vastleggen welke personen verantwoordelijk zijn voor het bijhouden van het verwerkingsregister.

Het is dus van belang om in eerste instantie goed vast te stellen of de organisatie verplicht is om een verwerkingsregister in te vullen en vast te leggen. U kunt hierin beter het zekere voor het onzekere nemen.

Voor meer details rondom het verwerkingsregister verwijzen wij u naar deze publicatie van Autoriteit Persoonsgegevens:
https://www.autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-europese-privacywetgeving/verantwoordingsplicht#ben-ik-verplicht-om-een-verwerkingsregister-op-te-stellen-7191

Boetebepaling
In maart 2019 heeft de Autoriteit Persoonsgegevens duidelijkheid verschaft met betrekking tot de boetebepaling. Autoriteit Persoonsgegevens handhaaft twee normen aan maximaal op te leggen boetes.
Categorie 1: Maximaal 10 miljoen euro of 2% van de wereldwijde jaaromzet voor het niet voldoen aan de verplichtingen van de AVG.

Categorie 2: Maximaal 20 miljoen euro of 4% van de wereldwijde jaaromzet bij het overtreden van de grondslagen van de AVG of het schenden van de privacy rechten van een persoon.
Het belangrijkste verschil tussen deze twee categorieën is dat categorie 1 een kwestie is van het correct vastleggen van processen en activiteiten rondom verwerking van persoonsgegevens en categorie 2 het schenden van de rechten (denk hier aan het zonder toestemming massaal verzamelen van (bijzondere) persoonsgegevens zonder een grondslag van verwerking). Belangrijk hier is dat Autoriteit Persoonsgegevens wel nu duidelijk aangeeft dat er ook rekening wordt gehouden met de onderneming.

De bakker om de hoek krijgt dus geen boete van 20 miljoen euro! Geen bangmakerij meer, maar in plaats daarvan duidelijke spelregels zodat we allen kunnen blijven ondernemen.
Voor meer informatie:
https://www.autoriteitpersoonsgegevens.nl/nl/nieuws/ap-past-boetebeleidsregels-aan

PRIVACYBELEID

Eén van de beste wijzen om inzichtelijk te maken dat uw organisatie voldoet aan de normen van de AVG is door het opstellen van een privacybeleid (en informatiebeveiliging). In dit beleid legt u de volgende zaken vast:

- Welke persoonsgegevens de organisatie (of per afdeling) verwerkt, inclusief de grondslag van verwerking.
- De processen rondom gegevensbescherming van de organisatie (per afdeling).
- De technische maatregelen die getroffen zijn om dataveiligheid te waarborgen.
- De richtlijnen waaraan de medewerkers zich dienen te voldoen (denk aan een clean desk policy). De Autoriteit Persoonsgegevens heeft inmiddels ook een aantal richtlijnen gegeven aan organisaties. In deze richtlijnen zijn een zestal aanbevelingen gedaan:
- Beoordeel of de organisatie verplicht is om een gegevensbeschermingsbeleid in te richten; niet iedere organisatie is dit verplicht. Dit is afhankelijk van de verwerking of uw organisatie.
- Gebruik interne en/of externe expertise; de functionaris gegevensbescherming kan hier als adviseur en intern toezichthouder een belangrijke rol in spelen.
- Leg het beleid vast in één document; voorkom versnippering van informatie in een privacyverklaring, een verwerkingsregister en een beleid.
- Wees concreet; een gegevensbeschermingsbeleid is een concrete vertaalslag van de AVG-normen naar de gegevensverwerkingen van een organisatie. Normen uit de AVG herhalen is niet voldoende.
- Maak het beleid bekend; publicatie van het gegevensbeschermingsbeleid is niet verplicht, maar maakt voor betrokkenen wel inzichtelijk hoe een organisatie met persoonsgegevens omgaat. Let bij de publicatie wel op met informatie over de beveiliging.
- Niet verplicht? Toch raadzaam; met een gegevensbeschermingsbeleid toont een organisatie aan de persoonsgegevens van betrokkenen te willen beschermen.

Voor meer informatie verwijzen wij u naar het volgende artikel:
https://www.autoriteitpersoonsgegevens.nl/nl/nieuws/zes-aanbevelingen-voor-een-privacybeleid

Privacy

Afsluitend

Privacybescherming is een belangrijk onderdeel geworden van het ondernemen, of we dit leuk vinden of niet. Het is belangrijk dat elke onderneming zelf in eerste instantie bepaalt hoe ver men wil gaan. Maak de risico's inzichtelijk, kijk naar de "verplichte checklist" en leg de acties vast welke er gedaan zijn rondom privacybescherming. Niet elk bedrijf hoeft een ISO27001 norm met nadruk op alle privacyvoorwaarden te hebben, net zo goed als dat Politie Nederland er niet mee wegkomt zonder alle verplichtingen op orde te hebben. Vooralsnog zal jurisprudentie duidelijke sturing geven aan deze wetgeving en zal daarmee de komende jaren meer duidelijkheid scheppen.

W.T. Privacy is een onderdeel van de W.T. Group

W.T. Privacy B.V.
Lentedans 51a 2907 AX Capelle a/d IJssel
Telefoon: +31 (0)10 285 79 90 email: info@wtprivacy.nl
www.wtprivacy.nl